What Is Claimed Is:

1. A method for conducting private secure electronic commerce comprising the steps of:

providing first and second sequences of encryption key material with said first sequence being suited for decrypting a message that has been encrypted using said second sequence and said second sequence being suited for decrypting a message that has been encrypted using said first sequence,

associating a value parameter with said first sequence,

providing said first sequence to an anonymous user in exchange for a payment,

providing encrypted data communications to said user until said value parameter is exhausted, and

adjusting said value parameter in response to said step of providing encrypted data communications.

2. The method as set forth in Claim 1 wherein said first and second sequences are identical one time pads.

3. The method as set forth in Claim 2 wherein said step of adjusting includes adjusting said value parameter in response to utilization of said one time pad of said first sequence such that when said one time pad is exhausted, said value parameter is exhausted.

4. The method as set forth in Claim 1 wherein said first sequence and said second sequence each include an identical plurality of sequentially arranged session keys.

5. The method as set forth in Claim 4 wherein said step of adjusting includes adjusting said value parameter in response to utilization of said session keys of said first sequence such that when said plurality of session keys is exhausted, said value parameter is

exhausted.

6. The method as set forth in Claim 5 wherein said step of providing encrypted data communications includes providing user initiated and user terminated connections to said user with said user utilizing a new session key from said plurality of session keys of said first sequence each time said user initiates a said connection.

7. The method as set forth in Claim 5 wherein said step of providing encrypted data communications includes the sub steps of:

providing user initiated and user terminated connections to said user,

monitoring a connection time that is the time that said user is connected, and

requiring said user to utilize a new session key from said plurality of session keys of said first sequence after a predetermined connection time.

8. The method as set forth in Claim 5 wherein said step of providing encrypted data communications includes recording a start time when said providing encrypted data communications first occurs, and requiring said user to utilize a new session key from said plurality of session keys of said first sequence at predetermined intervals after said start time.

9. The method as set forth in Claim 5 wherein said step of providing encrypted data communications includes monitoring a data quantity the is the number of bits of said communications and requiring said user to utilize a new session key from said plurality of session keys of said first sequence after a predetermined data quantity.

10. The method as set forth in Claim 1 wherein said step of providing encrypted data communications includes the substeps of:

receiving a message encrypted by use of said first sequence from said user,

decrypting at least a portion of said message by use of said second sequence, and

providing a service to said user in response to said message, and

adjusting said value parameter in response to providing said service.

11. The method as set forth in Claim 10 wherein said service is chosen from the group of information, software, goods, communication and calculation.

12. The method as set forth in Claim 1 including the step of providing anonymous network access to said user.

13. The method as set forth in Claim 1 including the step of providing encrypted application services to said user.

14. The method as set forth in Claim 1 wherein said step of providing encrypted data communications includes the substeps of:

generating a response to said user,

encrypting said response by use of said second sequence into an encrypted response,

sending said encrypted response to said user, and

adjusting said value parameter in response to said step of sending.

15. A method for conducting private secure electronic commerce comprising the steps of:

providing identical one time pad first and second sequences of encryption key material,

providing said first sequence to an anonymous user in exchange for a payment,

receiving a message encrypted by use of said first sequence from said user,

decrypting at least a portion of said message by use of said second sequence,

generating a response to said user,

encrypting said response by use of said second sequence into an encrypted response,

sending said encrypted response to said user, and

ceasing said sending and receiving when said first and second sequences have been completely used once.

16. A method for conducting private secure electronic commerce comprising the steps of:

providing first and second sequences of encryption key material with said first sequence being suited for decrypting data that has been encrypted using said second sequence and said second sequence being suited for decrypting a data that has been encrypted using said first sequence,

associating a value parameter with said first sequence,

providing said first sequence to an anonymous user in exchange for a monetary payment proportional to said value parameter,

providing encrypted application services to said user,

providing anonymous network access to said user,

adjusting said value parameter in response to said steps of providing encrypted application services and providing anonymous network access, and

ceasing said providing encrypted application services and said providing anonymous network access when said value parameter is exhausted.

17. A method for conducting private secure

electronic commerce comprising the steps of:

providing a first server,

providing to an anonymous first user, in exchange for a payment, a first sequence of encryption key material, an identifier associated with said first sequence, connection instructions for connecting to said server, and encryption instructions for encrypting and decrypting data using said first sequence,

providing to said server said identifier and a second sequence of encryption key material suitable for decrypting data that is encrypted with said first sequence and for encrypting data that can be decrypted with said first sequence, and

providing encrypted data communications between said first user and said first server.

18. The method as set forth in Claim 17 wherein said step of providing encrypted data communications includes the substeps of:

establishing a user initiated connection by said first user connecting to said first server by using said connection instructions,

receiving said identifier from said first user at said first server,

selecting said second sequence in response to receiving said identifier,

receiving, at said first server, from said first user, encrypted user data that said first user encrypted by using said first sequence and said encryption instructions,

decrypting at least a portion of said encrypted user data by using said second sequence,

encrypting server data by using said second sequence, and

transmitting from said first server, to said first user, said encrypted server data.

19. The method as set forth in Claim 18 further comprising the steps of:

providing third and fourth sequences of encryption key material with said third sequence being suited for decrypting a message that has been encrypted using said fourth sequence and said fourth sequence being suited for decrypting a message that has been encrypted using said third sequence,

providing said third sequence to said first server,

providing said fourth sequence to a second server,

after said step of decrypting at least a portion of said encrypted user data, encrypting said user data by using said third sequence and then transmitting, from said first server, to said second server, said encrypted user data, and

prior to said step of encrypting server data, receiving, at said first server, from said second server, encrypted server data that was encrypted by using said fourth sequence, and decrypting said encrypted server data by using said third sequence.

20. The method as set forth in Claim 17 further comprising the steps of:

establishing a first user account accessible to said first server with said first user account including said identifier and a first user value parameter that is proportional to said payment, and

adjusting said value parameter in response to said step of providing encrypted data communications.

21. The method as set forth in Claim 20 wherein:

said first server is an application service

provider,

said step of providing encrypted data communications includes said first server providing applications services to said first user, and

said step of adjusting includes adjusting said first user value parameter response to said providing applications services.

22. The method as set forth in Claim 21 wherein said applications services include no loss gambling with said first user value parameter being adjusted in response to said first user winning and losing, and with any loses by said first user being invested and payable at a predetermined future date.

23. The method as set forth in Claim 20 wherein:

said first server is an Internet service provider,

said step of providing encrypted data communications includes said first server providing anonymous Internet access to said first user, and

said step of adjusting includes adjusting said first user value parameter response to said providing Internet access.

24. The method as set forth in Claim 23 further including the steps of:

receiving a request for a service from said first user,

locating on the Internet a service provider that will provide said service,

establishing a service provider user account accessible to said first server including a service provider value parameter,

procuring said service for said first user from said service provider, and

adjusting said first user value parameter and said service provider value parameter in response to said step of procuring.

25. The method as set forth in Claim 20 wherein:

said first server is an email services provider,

said step of providing encrypted data communications includes said first server providing anonymous email services to said first user, and

said step of adjusting includes adjusting said first user value parameter response to said providing email services.

26. The method as set forth in Claim 17 wherein said step of providing to an anonymous first user includes providing a portable data storage device suitable for access by a data processing device to said first user, said storage device including said first sequence of encryption key material and said identifier as stored data, and said connection instructions and said encryption instructions as executable software.

27. A method of conducting secured electronic commerce through a server by a first user and said server, utilizing first and second sequences of encryption key material defining a pair of sequences in which each sequence of the pair is suited for decrypting data that has been encrypted using the other code sequence of the pair, comprising:

providing to said first user said first sequence,

providing to said encryption server said second sequence,

establishing an account accessible to said server, wherein said account tracks a value parameter associated with use of said encryption key material of at least said first sequence,

creating a first message by said first user,

encrypting said first message by use of said first sequence,

transmitting said encrypted first message by electronic means to said server,

decrypting at least a portion of said encrypted first message at said server by use of said second sequence,

accessing said account,

adjusting said value parameter of said account in response to use of said encryption key material of at least said first sequence.

28. The method of conducting secured electronic commerce of Claim 27 wherein:

said first sequence comprises a one time pad.

29. The method of conducting secured electronic commerce of Claim 27, wherein:

said value parameter for said first sequence comprises a monetary value, and

said step of adjusting said value parameter further comprises decreasing said monetary value in response to utilization of encryption key material in said step of encrypting said first message.

30. The method of conducting secured electronic commerce of Claim 27:

wherein said first message comprises a message body portion and a message address portion identifying an addressed recipient other than said server, and

further comprising:

after said step of decrypting, determining said addressed recipient, and

transmitting said message from said server to

said addressed recipient by electronic means.

31. The method of conducting secured electronic commerce of Claim 30, wherein:

said message body portion comprises preselected data,

said addressed recipient comprises a computer programmed to perform a calculation upon said preselected data and produce a result, and

further comprising:

creating a response message comprising a result portion containing said result,

transmitting said response message from said addressed recipient to said server by electronic means,

receiving said response message at said server, and thereafter encrypting at least said result portion of said response message using said second sequence of encryption key material;

transmitting said encrypted result portion of said response message from said server to said first user by electronic means.

32. The method of conducting secured electronic commerce of Claim 31 wherein said response message further comprises a fee portion indicating a value charged by said addressed recipient for producing said result.

33. The method of conducting secured electronic commerce of Claim 32, wherein:

said value parameter for said first sequence comprises a monetary value; and

said step of adjusting said value parameter further comprises decreasing said monetary value in response to said value charged by said addressed recipient for producing said result.

34. Apparatus for conducting secured electronic

commerce comprising:

a portable data storage device with stored data including a first sequence of encryption key material, and encryption software operable to encrypt and decrypt data by using said first sequence,

a server having a second sequence of encryption key material suitable for decrypting data that has been encrypted using said first sequence and encrypting data such that said data can be decrypted with said first sequence, and

a data processing device operable to connect to said portable data storage device, to access said stored data of portable data storage device, to execute said encryption software to encrypt and decrypt data by using said first sequence, to transmit data encrypted by using said first sequence to said server and to receive data encrypted by using said second sequence from said server.

35. Apparatus as set forth in Claim 34 wherein said portable storage device includes communications software operable by said data processing device to establish communications between said data processing device and said server.

36. A portable data storage device, suitable for operation with a data processing device, with stored data for conducting secured electronic commerce, comprising:

a first sequence of encryption key material suitable for decrypting data that has been encrypted by using a second sequence on a server and encrypting data such that said encrypted data can be decrypted by said server by using said second sequence,

encryption software suitable for execution by said data processing device to encrypt and decrypt data by using said first sequence,

an identifier associated with said first sequence for identifying said portable data storage device

to said server, and

connection software suitable for execution by said data processing device to connect said data processing device to said server for encrypted data communications therebetween.

37. The portable data storage device as forth in Claim 36 further comprising a value associated with said first sequence that is adjusted in response to utilization of said first sequence.

38. The portable data storage device as forth in Claim 36 further comprising a value associated with said identifier that is adjusted in response to services provided to said server and services provided by said server.